Usando servidores Radius com Produtos VPN3000

Índice

Introdução

Este documento descreve determinadas advertências encontradas ao usar alguns servidores Radius com o VPN 3000 concentrator e os clientes VPN.

- O servidor Radius do Windows 2000 exige o protocolo password authentication (PAP) autenticando um Cisco VPN Client. (Clientes de IPSec)
- Usar um servidor Radius que não apoie o protocolo microsoft challenge handshake authentication (MSCHAP) exige opções de MSCHAP ser desabilitado no VPN 3000 concentrator. (Clientes do [PPTP] do protocolo de tunelamento Point-to-Point)
- Usar a criptografia com PPTP exige os chaves MSCHAP-MPPE do retorno do atributo do RAIO. (Clientes de PPTP)
- Com Windows 2003, o MS-CHAP v2 pode ser usado, mas o método de autenticação deve ser ajustado como o “RAIO com expiração”.

Algumas destas notas apareceram nos Release Note do produto.

Antes de Começar

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Pré-requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco VPN 3000 Concentrator
- Cisco VPN Client

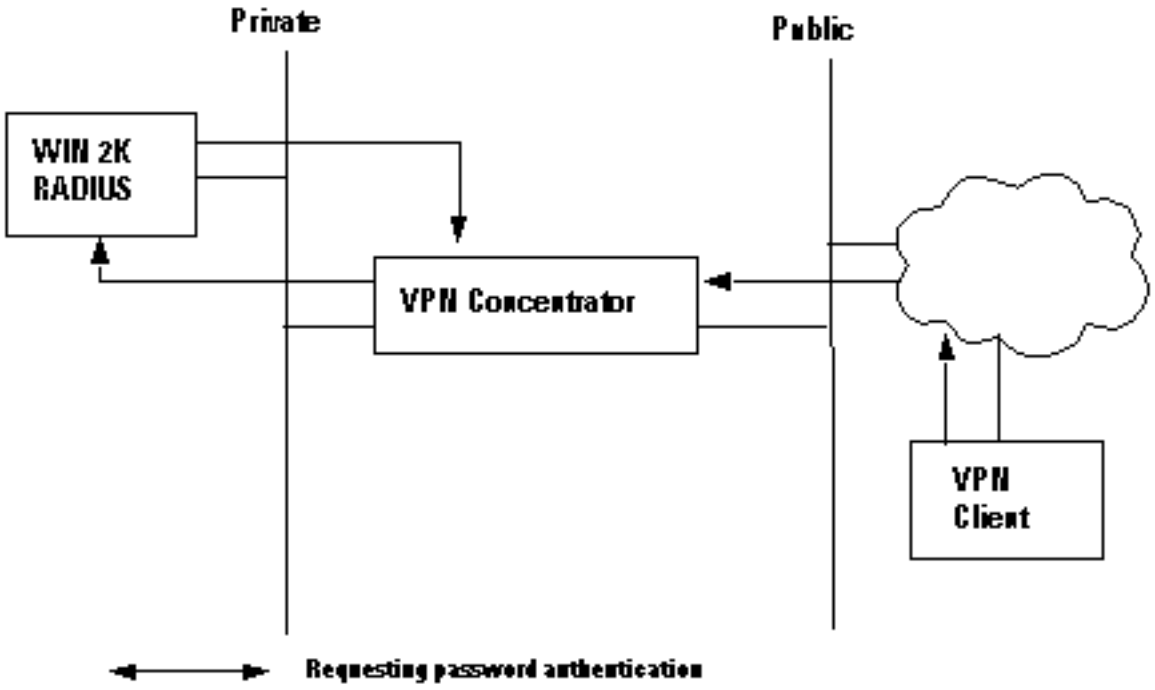
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Usando um servidor Radius do Windows 2000 para autenticar um Cisco VPN Client

Você pode usar um servidor Radius do Windows 2000 para autenticar um usuário de cliente VPN. Na seguinte encenação (o cliente VPN está pedindo a autenticação), o VPN 3000 concentrator recebe um pedido do cliente VPN que contém o nome de usuário e senha do usuário cliente. Antes de enviar o username/senha a um servidor Radius do Windows 2000 na rede privada para a verificação, o concentrador VPN pica-a, usando o algoritmo HMAC/MD5.

O servidor Radius do Windows 2000 exige o PAP autenticando uma sessão de cliente VPN. Para permitir o servidor Radius de autenticar um usuário de cliente VPN, verifique o parâmetro da **autenticação não criptografada (PAP, SPAP) no** indicador do **perfil do discado da edição** (à revelia, este parâmetro não é verificado). Para ajustar este parâmetro, selecione a **política de acesso remoto que** você se está usando, **propriedades** seletas, e selecione a aba da **autenticação**.

Note que a palavra *Unencrypted n*este nome de parâmetro é enganadora. Usar este parâmetro não causa uma ruptura de segurança, porque quando o concentrador VPN envia o pacote de autenticação ao servidor Radius, não envia a senha na claro. O concentrador VPN recebe o username/senha e os pacotes criptografado do cliente VPN, e executa uma mistura HMAC/MD5 na senha antes de enviar o pacote de autenticação ao server.



Usando um servidor RADIUS que não suporte MSCHAP

Alguns servidores Radius não apoiam a autenticação de usuário MSCHAPv1 ou MSCHAPv2. Se você está usando um servidor Radius que não apoie o MSCHAP (v1 ou v2), você deve configurar o protocolo de autenticação de PPTP do grupo base para usar o PAP e/ou RACHAR e desabilitar igualmente as opções de MSCHAP. Os exemplos dos servidores Radius que não apoiam o MSCHAP são o servidor Radius de Livingston v1.61 ou todo o servidor Radius baseado no código de Livingston.

Nota: Sem MSCHAP, os pacotes a e dos clientes de PPTP não serão cifrados.

Utilizando criptografia com PPTP

Para usar a criptografia com PPTP, um servidor Radius deve apoiar a autenticação MSCHAP e deve enviar os chaves MSCHAP-MPPE do retorno do atributo para cada autenticação de usuário. Os exemplos dos servidores Radius que apoiam este atributo são mostrados abaixo.

- Cisco Secure ACS for Windows - versão 2.6 ou mais recente
- Funk Software Steel-Belted RADIUS
- Servidor de autenticação de Internet do microsoft no bloco das opções Server NT4.0
- Microsoft Commercial Internet System (MCIS 2.0)
- Microsoft Windows 2000 Server -- Internet Authentication Server

Informações Relacionadas

- Página de suporte RADIUS
- Cisco Secure ACS para página de suporte do Windows
- Página de suporte do Cisco VPN 3000 Series Concentrator
- Página de suporte ao cliente do Cisco VPN 3000 Series
- Página de suporte do IPSec

- Página de suporte do PPTP
- RFC 2637: Protocolo de túnel ponto-a-ponto (PPTP)
- Solicitações de Comentários (RFCs)
- Suporte Técnico - Cisco Systems